Claims:

1. A system for evaluating a proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness, comprising:

a generator supplied with a third random tape, for generating a common input and a witness from the third random tape based on a predetermined function, wherein it is difficult to use the predetermined function to calculate a witness from a common input;

a simulator supplied with a fourth random tape; and

a distinguisher supplied with a fifth random tape, wherein

the generator supplies the common input to the prover, the verifier, the simulator and the distinguisher, and supplies the witness to the prover and the distinguisher;

a proof history is generated with involving the prover;

a simulated proof history is generated by the simulator without involving the prover; and

the distinguisher evaluates the proof system depending on whether a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs and computationally distinguishable for at least one of the possible common inputs.

2. The system according to claim 1, wherein

the proof history is generated by the verifier interacting with the prover using the second random tape and the common input, the proof history including the second random tape and the interactive data with the prover,

the simulated proof history is generated by the simulator that supplies a sixth random tape to the verifier and interacts with the verifier to simulate interaction between the prover and the verifier, the simulated proof history including the sixth random tape and the simulated interactive data.

3. The system according to claim 1, wherein

the prover comprises a proving section and a hash function section, wherein the hash function section inputs data from the proving section and outputs hash data of the inputted data back to the proving section,

the proof history is generated by the prover in which the proving section interacts with the hash function section to produce interactive data and hash data of the interactive data is replaced with random data, wherein the proof history further includes data transferred from the prover to the verifier,

the simulated proof history is generated by the simulator that simulates interaction between the prover and the verifier based on the common input and the fourth random tape, the simulated proof history including the simulated interactive data.

4. The system according to claim 1, wherein, if for every distinguisher a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs to an extent of an approximately 100% probability and computationally distinguishable for the remaining part of the common inputs, it is determined that the proof system is classified under a weakly computational zero-knowledge proof class.

5. The system according to claim 1, further comprising:

a memory for storing an evaluation result of the proof system obtained by the distinguisher, wherein the evaluation result is on public view.

6. The system according to claim 5, wherein the evaluation result stored in the memory is accessible through a network.

7. A method for evaluating a proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness, comprising:

generating a common input and a witness uniformly and randomly from a third random tape based on a predetermined function, wherein it is difficult to use the predetermined function to calculate a witness from a common input;

supplying the common input to the prover, the verifier, the simulator and the distinguisher;

supplying the witness to the prover and the distinguisher;

generating a proof history with involving the prover;

generating a simulated proof history by the simulator without involving the prover; and

evaluating the proof system depending on whether a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs and computationally distinguishable for at least one of the possible common inputs.

8. A proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness, comprising:

a generator supplied with a third random tape, for generating a common input comprising g, h, $y = g^x$, and z′ and a witness comprising x from the third random tape, wherein x is an integer and g, h and z′ are elements of a group which is previously determined and has an order thereof, wherein the prover inputs the common input and the witness from the generator and the verifier inputs the common input from the generator;

wherein, after interaction between the verifier and the prover starts, the following steps are performed:

A) the verifier uniformly and randomly selects an integer b smaller than the order of the group and a challenge c from the second random tape, generates a challenge commitment $a = g^b y^c$, and sends the challenge commitment a to the prover;

B) the prover uses the first random tape to uniformly and randomly select d, e and f, which are integers smaller than the order of the group, calculates

$h' = h^d$,

$w' = z'^d$,

$v = h^{xd}$,

$y' = g^e$,

$v' = h'^c$,

$h'' = h^f$, and

$w'' = z'^f$

and sends h', w', v, y', v', h'' and w'' to the verifier;

C) the verifier sends the integer b and the challenge c to the prover;

D) the prover determines from the received b and c whether $a = g^b y^c$ is satisfied and, if not satisfied, then the interaction is terminated and, if satisfied, then the interaction continues;

E) the prover uses the integers d, e and f and the witness to calculate response r and r′ and send them to the verifier:

$r = xc+e \bmod$ (the order of the group); and

$r' = dc+f \bmod$ (the order of the group);

F) the verifier uses the h′, w′, v, y′, v′, h′′ and w′′ received from the prover, the response r and r′, the challenge c, and the common input p, q, g, h, y, z′ to determine whether a set of following expressions is satisfied:

$g^{r} = y^{c}y'$,

$h'^{r} = v^{c}v'$,;

$h^{r'} = h'^{c}h''$,

$z'^{r'} = w'^{c}w''$, and

$v' \neq w'$,

and, if the set of following expressions is satisfied, then the verifier accepts the proof and, if at least one expression is not satisfied, then the verifier denies the proof.

9. A program instructing a computer to evaluate a proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness, the program comprising the steps of:

generating a common input and a witness uniformly and randomly from a third random tape based on a predetermined function, wherein it is difficult to use the predetermined function to calculate a witness from a common input;

supplying the common input to the prover, the verifier, the simulator and the distinguisher;

supplying the witness to the prover and the distinguisher;

generating a proof history with involving the prover;

generating a simulated proof history by the simulator without involving the prover; and

evaluating the proof system depending on whether a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs and computationally distinguishable for at least one of the possible common inputs.

10. A program instructing a computer to implement a proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness, the program comprising the steps of:

generating a common input comprising g, h, $y = g^x$, and z′ and a witness comprising x from the third random tape, wherein x is an integer and g, h and z′ are elements of a group which is previously determined and has an order thereof, wherein the prover inputs the common input and the witness from the generator and the verifier inputs the common input from the generator;

after interaction between the verifier and the prover starts,

A) the verifier uniformly and randomly selecting an integer b smaller than the order of the group and a challenge c from the second random tape, generating a challenge commitment $a = g^b y^c$, and sends the challenge commitment a to the prover;

B) the prover using the first random tape to uniformly and randomly select d, e and f, which are integers smaller than the order of the group, calculating

$h' = h^d$,

$w' = z'^d$,

$v = h^{xd}$,

$y' = g^e$,

$v' = h'^c$,

$h'' = h^f$, and

$w'' = z'^f$

and sending h', w', v, y', v', h'' and w'' to the verifier;

C) the verifier sending the integer b and the challenge c to the prover;

D) the prover determining from the received b and c whether $a = g^b y^c$ is satisfied, wherein if not satisfied, then the interaction is terminated and, if satisfied, then the interaction continues;

E) the prover using the integers d, e and f and the witness to calculate response r and r' and sending them to the verifier:

$r = xc+e \bmod$ (the order of the group); and

$r' = dc+f \bmod$ (the order of the group);

F) the verifier using the h', w', v, y', v', h'' and w'' received from the prover, the response r and r', the challenge c, and the common input p, q, g, h, y, z' to determine whether a set of following expressions is satisfied:

$g^{r} = y^{c}y'$,

$h'^{r} = v^{c}v'$,;

$h^{r'} = h'^{c}h''$,

$z'^{r'} = w'^{c}w''$, and

$v' \neq w'$,

wherein if the set of following expressions is satisfied, then the verifier accepts the proof and, if at least one expression is not satisfied, then the verifier denies the proof.

11. A proof system comprising a prover supplied with a first random tape and a verifier supplied with a second random tape, wherein the prover communicates with the verifier to prove that the prover has a witness, wherein the proof system is determined by an evaluator that it is included in a weakly computational zero-knowledge proof class, the evaluator comprising:

a generator supplied with a third random tape, for generating a common input and a witness from the third random tape based on a predetermined function, wherein it is difficult to use the predetermined function to calculate a witness from a common input;

a simulator supplied with a fourth random tape; and

a distinguisher supplied with a fifth random tape, wherein

the generator supplies the common input to the prover, the verifier, the simulator and the distinguisher, and supplies the witness to the prover and the distinguisher;

a proof history is generated with involving the prover;

a simulated proof history is generated by the simulator without involving the prover; and

the distinguisher determines that the proof system is included in the weakly computational zero-knowledge proof class, when a difference in distribution between the proof history and the simulated proof history is computationally indistinguishable for a great majority of possible common inputs and computationally distinguishable for at least one of the possible common inputs.